Federal Computer Incident Response Center

The FedCIRC Bits & Bytes

A quarterly newsletter for Information System Security Managers/Officers & System Administrators

January 2003

TechNotes

Can You Manage?

On the long checklist of vital issues for IT managers, the box labeled "enterprise security" always calls for special attention. Not long ago, major threats to information systems consisted of an occasional virus, worm, or clever intruder, and it was relatively easy to check off the enterprise security box and continue down the list.

Today, however, the threats are much larger, and the stakes are much higher. Inevitably, when the pencil stops at the enterprise security box, the nagging question remains: "Can we really manage IT security on our own?"

Not surprisingly, more and more organizations in both the public and private sectors are answering "no" and turning to Managed Security Service Providers (MSSPs) to provide the technical expertise and sophisticated protection needed for today's enterprise environments.

Taking off

According to Allan Carey, program manager, Information Security Services, IDC Inc., the U.S. market for managed IT security services reached approximately $720 million in 2000, and will climb to $1.9 billion by 2005, growing about 23 percent annually.

"Customers want information security solutions that ensure scalability, seamlessly integrate into the network, and provide a measurable return on investment," Carey said. "The MSSP market is being driven by the need of various organizations to augment constrained internal resources, as well as leverage a service provider whose core competency is security."

More organizations are turning to MSSPs because, "an MSSP offers services where the sole focus of the company is security," Carey said. "A more general IT outsourcing vendor typically provides a broader array of services with less specialization, and may not be able to offer the same level of security expertise as an MSSP. The MSSP approach benefits organizations in the long run through reduced operational costs and the ability to better allocate internal IT security resources to initiatives with strategic importance," Carey observed.

Carey points out that private industry led the way in adopting MSSPs, but the government market is starting to pick up steam. "It has taken a tremendous amount of education and awareness about the increasing business risks and the benefits of outsourcing to get the market where it is today," Carey said.

Getting on board

Grant Geyer, director, Managed Security Services, Symantec Corp., concurs with Cary's assessment, and adds that, "When it comes to MSSPs, we're seeing a tremendous amount of interest, as well as a greatly increased adoption rate, from public sector organizations." The primary factors currently driving the market for MSSPs include:

- Growing complexity of networking technology.
- The need for real time analysis and processing of firewall and alert data.
- A variety of operating systems, and versions of operating systems, installed throughout enterprises.
- Ability to augment constrained internal resources.
- The chance to leverage a service provider whose core competency is IT security.
- Application software packages that address security lightly, or not at all.

- Increased numbers of hackers, as well as the easy availability and sophistication of hacking tools.
- The opportunity to lower total cost of ownership and increase return on investment.
- Significant increase in reported incidents of worms, viruses, and blended threats.

More vulnerabilities that can be exploited by hackers are being found on operating systems every week," Geyer warned. "The problem is getting worse, not better. It's like having so many doors and windows on your house you can't protect them all."

What's more, the lag time between a vulnerability being discovered and a hacker exploiting it keeps shrinking. "It used to be upwards of a year before an operating system exploit was available," Geyer said. "Now it's only a matter of weeks, sometimes days."

Filling the void

As complex information systems spread throughout distributed enterprises, many organizations addressed IT security by implementing commercial-off-the-shelf (COTS) firewalls and antivirus software. While this blocked certain types of common attacks and provided a logging and reporting mechanism for IT managers, it didn't provide proactive capabilities or an immediate defense against security breaches. What's more, standard intrusion detection systems (IDSs) generated a significant number of false positives, each of which required scarce manpower to investigate.

When IT outsourcing picked up,Managed Service Providers began offering firewall management as one of their services. They made sure the firewall was up and running, installed operating system patches, made some occasional rule changes, and provided monthly reports on log traffic. However, in many cases, security breaches and hacking incidents were handled after the fact, leaving organizations vulnerable and only able to repair damage after it had occurred. Few were able to prevent attacks, or stop them while they were underway.

For that to happen, the managed providers had to provide round-the-clock security monitoring and real time data analysis, something that few could afford to offer. This void was filled by MSSPs, where highly trained security professionals draw on the resources, expertise, and infrastructure needed to continually monitor enterprise systems and protect against attacks.

A real shocker

As the MSSP market took off, Geyer found that implementing managed IT security services could be an eye-opener. "The scary part was that many organizations didn't even know they had been broken into," he said. "We would turn on our service and discover that not only had the information system been breached, but attacks on other companies or organizations were being launched from their servers."

That's not likely to happen with an MSSP on board, however, because all suspicious events are flagged and immediately sent to skilled analysts who can initiate corrective action. Clients are notified concerning the severity of the event, and guided through the steps necessary to protect the system. Leading MSSPs can also store large amounts of security-related data in their operations centers and use it for long-term trending and analysis. Some even have access to global databases of known violators, which can help identify troublemakers when attacks occur. "Technology is not enough to provide comprehensive protection," Geyer emphasized. "You need an analytical process, immediate access to highly skilled expertise, and the resources necessary to correlate and analyze all the different security alarms that these technologies can generate."

As cyberspace becomes an increasingly dangerous place, Geyer expects to see a growing demand for MSSPs. "MSSPs have proven they have a viable business model, they're sustainable and scalable, and companies and government organizations have recognized that they can trust them," he said.

Sidebar one: Evaluation Criteria for MSSPs

Scalability - MSSPs must be able to capture and analyze large amounts of security data for systems of all sizes, from office workgroups to global enterprises.

Neutrality - It is vital that the MSSP be product-neutral and capable of supporting a full range of IT security products, regardless of the originating vendor.

Stability - The MSSP should be able to demonstrate a long-term financial commitment to the MSSP market, as well as a track record of providing managed IT security services to enterprise organizations.

Scope of operations - A global reach and access to leading industry intelligence are key assets of an effective MSSP.

Superior service - Look for competitive, performance-based service level agreements (SLAs) where security isn't sacrificed for other considerations. Settle for no less than enterprise-wide, real time security monitoring, 24/7/365.

Staff interaction - Most IT organizations possess some in-house security expertise. A seasoned MSSP knows how to augment, not replace, that expertise.

Skills and tools - The MSSP should have the best security analysts available, and they should be armed with real time access to sophisticated query tools, data, and analytical capabilities. COTS software can't do it all. Ask about specialized data mining and analysis tools the MSSP can develop to protect your unique environment.

Sidebar 2: Key Questions for the MSSP

Will the MSSP fit comfortably into your existing IT outsourcing arrangement and be able to work with other contractors and in-house IT security staff?

Can the MSSP implement responsive forensics in real time, or is there a delay in how quickly they can respond to attacks and threats?

Is the MSSP relying strictly on commercial-off-the-shelf (COTS) technology, or have they developed data mining and correlation engines that go beyond the capabilities of shrink-wrapped products?

Will the MSSP invite you onto the shop floor to "look under the hood" of the technologies it will use to protect your IT environment?

Will the MSSP supply customer references and encourage you to talk to them?

15 Facts About Blended Threats

Anyone tasked with maintaining or protecting information systems or enterprise networks should be familiar with the most important aspects of blended threats, the most insidious and destructive form of malicious computer hacking to appear so far. When it comes to blended threats, experts agree on two things: those that were launched in the recent past caused significant damage which cost millions of dollars to repair, and those that may be launched in the near future will likely be much worse.

1. A blended threat is a malicious computer program that uses multiple techniques to spread among systems.
2. Before long, blended threats may incorporate 10 to 20 methods of propagation instead of the four or five used so far.
3. The primary goal of blended threats, and those who implement them, is to cause as much damage as possible to as many systems as possible, as quickly as possible.
4. Payloads carried by blended threats will likely become more damaging, resulting in more corruption and destruction of data and denials of service.
5. Three of the most infamous blended threats to attack corporate and government computer systems were CodeRed, CodeRed II, and Nimda.
6. CodeRed II left behind a "back door" program that could provide hackers with access to an infected server or PC, allowing them to return later and do even more damage.
7. Blended threats can replicate very rapidly and infect systems where other viruses would be stopped.
8. Hackers use known software vulnerabilities, web page downloads, and email attachments to spread blended threats. User vigilance is essential in combating blended threats.
9. CodeRed attacked the White House web site, but was unsuccessful in causing any damage. So far, blended threats have not targeted any specific corporation or government agency, but IT security experts are bracing for a targeted attack.
10. The increased use of broadband connections will amplify the power and impact of blended threats exponentially. Before long, attacks may be launched from millions of home PCs, in addition to corporate and government computers.
11. Users must be proactive when confronted with the possibility of exposure to blended threats. Patches were available for some of the vulnerabilities exploited by CodeRed, CodeRed II, and Nimda before they were launched, but many people did not implement them. Organizations that kept their security patches current, however, were not impacted by those threats.
12. An effective way to protect against blended threats is to implement comprehensive security measures at all levels, including the gateway, server, and client. An intrusion detection solution can also help thwart blended threats by alerting administrators that an attack is taking place.
13. Automated vulnerability management and assessment software can help assess a system's vulnerability to blended threats by launching a simulated attack and alerting administrators to the weak spots in the system.

14. Blended threats are also called evolving threats, mixed threats, and integrated or complex threats.

15. Blended threats must be identified and removed as quickly as possible. Potential incursions must be blocked by the firewall if at all possible. Network and host computers should be monitored for improper activity 24/7 to protect against blended threats.

**These articles were written by Claude Bauer, Symantec Corporation*

Latest FedCIRC Advisories

FedCIRC Advisory FA-2002-36
Multiple Vulnerabilities in SSH Implementations

FedCIRC Advisory FA-2002-35
Vulnerability in RaQ 4 Servers

FedCIRC Advisory FA-2002-34
Buffer Overflow in Solaris X Window Font Service

FedCIRC Advisory FA-2002-33
Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)

FedCIRC Advisory FA-2002-32
Backdoor in Alcatel OmniSwitch AOS

FedCIRC Advisory FA-2002-31
Multiple Vulnerabilities in BIND

FedCIRC Advisory FA-2002-30
Trojan Horse tcpdump and libpcap Distributions

The FedCIRC Bits & Bytes Newsletter

Editor
Corliss A. McCain

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions for the next issue is March 1, 2003. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service